DOCUMENT RESUME

ED 383 011 CS 508 918

AUTHOR Penkoff, Diane
TITLE Public Flames and Private Fantasies: When Is Computer-Mediated Communication Private?
PUB DATE 26 Feb 94
NOTE 13p.; Paper presented at the Annual Meeting of the Western States Communication Association (65th, San Jose, CA, February 23-27, 1994).
PUB TYPE Speeches/Conference Papers (150) -- Information Analyses (070)

EDRS PRICE MF01/PC01 Plus Postage.
DESCRIPTORS *Communication Research; *Computer Mediated Communication; Ethics; *Freedom of Speech; Higher Education; Literature Reviews; *Privacy; Research Needs; Technological Advancement
IDENTIFIERS *Communication Behavior

ABSTRACT

Noting that corporations and academic institutions are struggling with issues of balance between system security and freedom of speech, this paper reviews current literature concerning privacy in computer-mediated communication (CMC) from the perspectives of both the individual user and the system administration. Focusing on the communicative rather than the technical aspects of CMC, the paper considers personal rights to privacy and freedom of expression, weighed against system administrator liabilities and responsibilities to users. The paper notes that system administrators and owners of academic systems join private and corporate sectors in walking an ethical and legal tightrope and notes that researchers, apart from legal considerations, are wrestling with the ethics and moral responsibilities of sampling text from public bulletin boards and mailing lists. The paper suggests that users engage in risky communication in spite of system limitations for security and privacy. The paper concludes that CMC is evolving minute-by-minute, offering communication scholars new opportunities for research with every new development. (Contains 54 refrences.) (RS)

****
* Reproductions supplied by EDRS are the best that can be made *
* from the original document. *
****

"PERMISSION TO REPRODUCE THIS MATERIAL HAS BEEN GRANTED BY
D. Penkoff
TO THE EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)."

ED 383 011

Public Flames and Private Fantasies: When is Computer-Mediated Communication Private?

Diane Penkoff
Department of Communication Arts & Sciences
University of Southern California

Presented to
Western States Communication Association
Mass Communication Interest Group
San Jose, CA
February 26, 1994

U.S. DEPARTMENT OF EDUCATION
Office of Educational Research and Improvement
EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)
✓ This document has been reproduced as received from the person or organization originating it.
☐ Minor changes have been made to improve reproduction quality.
• Points of view or opinions stated in this document do not necessarily represent official OERI position or policy.

Diane Penkoff currently is
Assistant Professor of Communication
Purdue University
1366 Liberal Arts & Education Building, 2114
West Lafayette, IN 47907-1366
Internet: penkoff@sage.cc.purdue.edu

Abstract

This paper reviews current literature concerning privacy in computer-mediated communication (CMC), from the perspectives of both the individual user and the system administration. It considers personal rights to privacy and freedom of expression, weighed against system administrator liabilities and responsibilities to users. The literature suggests that users engage in risky communication in spite of system limitations for security and privacy. Questions are raised concerning risky communication behaviors in light of probable user knowledge that CMC is not private.

Public Flames and Private Fantasies: When is Computer-Mediated Communication Private?

> The communication takes place in what is described as Cyberspace -- a global nervous system that is entered through a computer keyboard, connecting to millions of people around the world by radio waves and fiber optic cables (Baird, 1991).

Whether we're dealing with a small, local system, or the estimated seven million people around the world who inhabit cyberspace each day (Baird, 1991), the concepts of what is public and what is private are muddy in computer-mediated communication (CMC). The purpose of this paper is to review current literature concerning privacy in CMC, from the perspectives of both the individual user and the system administration, considering personal rights to privacy and freedom of expression, weighed against system liabilities and responsibilities to their users. This paper focuses on the communicative rather than the technical aspects of computer-mediated communication, thus, it does not address problems of system security and protection from worms, viruses, or Trojan horses, nor does it tackle the complex problems of

CS508918

BEST COPY AVAILABLE

confidentiality in the context of public and private databases (e.g., financial status reports, employee personnel files, software piracy, etc.). This review does encompass all commonly-used forms of computer-mediated communication, including electronic mail, bulletin board services, and computer teleconferencing and "chatting."

From fliers to fiber optics: new technology brings new challenges

Once upon a time, people posted important messages on trees and church doors, and letters were delivered by hand. Today, people still post messages on bulletin boards on kiosks and in supermarkets, employee lounges, and convention centers, and letters are delivered by mail or courier services. With the advent of the personal computer (PC), relatively new methods have appeared for these age-old forms of communication: the electronic bulletin board (BBS) and electronic mail (e-mail). While public bulletin boards typically are read by groups of people who share similar interests, e-mail can be used to communicate one-to-one or one-to-many.

Person-to-person, "private" electronic mail is the computerized equivalent of correspondence in the U.S. Postal system. The communicator composes a message and sends it via computer network to a recipient or several recipients at other locations. But unlike the postal system, or the telephone system, for that matter, the law does not fully protect privacy of e-mail. User accounts are protected under the Electronic Communications Privacy Act (ECPA) of 1986, which amends the federal wiretap law and makes accessing stored electronic messages by breaking into an electronic system or exceeding authorized access a criminal offense (Hernandez, 1987). But any manager, investigator, or system administrator ("sysop") with global access to the computer system ("God powers") is capable of monitoring an electronic message. It is the naive user who ignores the reality that somehow, somewhere, someone can read privately posted messages -- unknown to the sender.

Some systems, most notably CompuServe, have a reputation for maintaining correspondent privacy. Pornographic scanned, full-color photographs are sent with great abandon and enthusiasm between some CompuServe subscribers with no recrimination nor interest from CompuServe staff. Other systems, apparently valuing standards over privacy, go so far as to censor "private" messages. The widely-used Prodigy network, for example, has been under fire for maintaining a policy of censorship (Lewis, 1990, p. F8). But the issue of privacy is problematic for all systems. Indeed, "system administrators seeking to deliver misaddressed electronic mail can hardly avoid reading the messages" (Turner, 1991, p. A13). Miller (1992, p. p8F(N) suggests that employees should "assume [e-mail security] ...doesn't exist." In other words, the term, "e-mail privacy," is an oxymoron.

Messages on public bulletin boards are the electronic counterparts to those pinned on physical bulletin boards. They are posted for all to see who care to look. Some systems permit "private" messages on the bulletin boards, which makes them invisible to the casual reader, but readable to the intended recipient. One might say they are posted on

the bulletin board in electronic envelopes, which, although sealed, are by no means secure. Clearly, the security of both forms of electronic communication is questionable, particularly if not encrypted -- and most e-mail messages are not.

Beyond asynchronous e-mail and bulletin board capabilities, many computer networks and systems support synchronous ("real time") computer teleconferencing. Typically, teleconferencing is open to anyone who logs on and enters the command to enter a "chat." Often, however, users also can create "private" teleconferences, accessible to other users only by invitation. The Internet Relay "Chat" (IRC) supports teleconferences, both private and public -- a number with adult or pornographic themes.

Where does system responsibility end and user right to privacy begin? Kahn (1989) describes the all-too-common phenomenon of a computer user dialing up a local BBS, logging in with her secret password, and being "deluged with lewd electronic mail from complete strangers and hostile messages from persons with whom she believed she was on friendly terms" (page 1). The BBS user eventually realizes she is the victim of a computer "hacker" or "phreaker;" her password was pirated, and someone has been electronically impersonating her. During the last few months, a similar incident occurred locally, on the university BBS. A regular user's password was discovered by a hostile hacker, who logged on several times a day, leaving violent, racist and sexist, public and private messages. It was several days before other BBS users alerted the sysop, who deleted the phreaker's bogus account from the system and contacted the individual who was being impersonated.

Let's assume our local BBS user is enraged by the public humiliation of the offensive public messages. Is he justified in suing the sysop and/or the owner of the BBS for defamation? Most BBS's, the university BBS included, are run at a loss by volunteers (Riddle, 1990). Must the sysop monitor all messages and be responsible for those in poor taste or of a defaming nature? High volume boards make message-by-message monitoring nearly impossible.

Many organizations, including academic institutions, are struggling with issues of balance between system security and system standards vs. freedom of speech and privacy. This problem is made thornier by the popularity of e-mail lists, often with huge memberships, that are devoted to adult topics. On the Internet, for example, four of the fifteen most popular news groups focus on sexual topics, including erotic arts, stories, and bondage (Reid, July 1993). Turner (1991, p. A13) notes that in local, university-owned systems, "The kinds of messages once limited to lavatory walls are now causing problems on campus computer networks -- for reasons that may have as much to do with technology as with moral standards."

Privacy difficulties arise from user error, as well as from external monitoring. The user always is a mere keystroke away from disaster, and can send a message to the wrong party, or even to large groups of people, with a single typographical slip-up, as illustrated by the following case:

> One job-seeker mistakenly sent his resume and a letter to a 1,000-person mailing list rather than to the hiring manager, [inadvertently] divulging salary demands and why he wanted the job (Keubelbeck, 1991, p. E2).

Anyone using computer-mediated communication undoubtedly is aware of the flurries of media attention paid to the issue of security and privacy in electronic mail systems (e.g., Anderson, Johnson, Gotterbarn, & Perolle, 1993; Keppel, 1990; Moore, 1992; Reynolds, 1990). Organizations and individual users, alike, are discovering the complexities of communicating in a unique medium. Horror stories abound (e.g., Lewis, 1990; Solomon, 1990; Keubelbeck, 1991):

* Bonita B. Bourke and Rhonda L. Hall sued Nissan Motor Corporation of USA in Carson, CA. They alleged that their manager "electronically eavesdropped" on their e-mail and that they were fired after filing a grievance over it. (White, 1991, p. D3).

* Epson America was slapped with two lawsuits for invasion of privacy. One was filed by a former e-mail manager who alleged she was fired for trying to stop company managers from reading e-mail messages between employees (Burke, 1990, p. 124; Keubelbeck, 1991, p. E2).

* Lotus Development Corporation canceled its development of the software package, "Lotus Marketplace," a market research and direct marketing package that included an electronic database, due to mounting concern that it placed excessive power in the hands of small businesses, creating invasions of privacy. (Francese, 1991; Miller, 1991, p. B1).

* In the wake of the infamous Rodney King beating, a number of Los Angeles Police officers experienced, first-hand, the archival nature of electronic communication. In the process of investigating the incident, Christopher Commission studied squad car messages and characterized approximately 700 of them improper and "apparently racist or sexist" (Keubelbeck, 1991, p. E2).

Michael F. Cavanagh, executive director of the Electronic Mail Association in Arlington, VA, sees the problem as one of balance:

> The juxtaposition of that LAPD situation and the public's right to know what was on the tapes with the issue of how to have a secure workplace illustrates how complex the issue is (Keubelbeck, 1991, p. E2).

The corporate sector toes a similar fine line between electronic supervision of employees and invasion of their rights. Miller (1992)

notes that although it's against the law for organizations to monitor employee telephone conversations, even on a company-owned phone, the regulations concerning e-mail are less clear. A case that may change this is reported by Kapor (1992) and Ratcliffe (1992) concerning Borland International, Inc. and Symantec Corporation. Eugene Wang, a Borland employee, left the company to join Symantec. Borland claims to have found memos in Wang's MCI mail to Symantec--memos written prior to Wang's departure that include Borland proprietary information. When Borland executives turned over Wang's mail messages to local police, the messages were used to obtain search warrants to enter Wang's home and that of Gordon Eubanks, the Symantec chief executive officer. Ratcliffe (1992) speculates that Wang and Eubanks would argue violation of the ECPA, although Borland indicates that as owner of the account, the search was legal. Kapor points out that although current law protects messages while they are in transmission over public services, this case may help define the degree to which employers can search employees' stored e-mail messages.

Gender issues, too, are emergent in organizational computer-mediated communication. One case study that appears in Harvard Business Review raises the issue of an employee being sexually harassed by a superior. The dilemma: if a manager discovers evidence of such harassment in the employee's electronic mailbox, at what point between reporting the incident and protecting the employee's right to privacy does justice lie (Niven, Wang, Rowe, Taga, Vladeck, & Garron, 1992)?

System administrators and owners of academic systems join private and corporate sectors in walking an ethical and legal tightrope. Apparently valuing intellectual freedom and the right to free expression, they still have to weigh security with freedom:

System security takes priority over privacy at most [scholarly] institutions, although most colleges and university [sic] do not compromise privacy lightly. Most require system administrators to check with university officials--often up to the level of a vice-president or provost--before reading a user's account (Turner, 1991, p. A13).

As technological advances continue, the legal, ethical, and moral issues intensify.

Desperately seeking solutions

A number of authors are grappling with legal and ethical solutions for privacy issues in computer mediated communication. Anderson, et al. (1993) describe nine case studies for applying the Code of Ethics of the Association for Computing Machinery (ACM) in practice. Included in the Code are stipulations requiring that unauthorized or inappropriate access to data be prevented, and that organization leaders should determine if systems are adequate to protect privacy. In response to consumer concerns, software companies are designing programs to keep e-mail private. Two new titles, for example, are "Privacy Enhanced Mail" and "Pretty Good Privacy" (Wallich, 1993). One proposed solution in dealing with electronic evidence of sexual

harassment involves coaching the employee in handling the situation (Niven, Wang, Rowe, Taga, Vladeck, & Garron, 1992). But employees still have a right to know that their electronic correspondence may be monitored. Loebl (1992) suggests that employers can deal, at least in part, with employees' privacy issues by including an addendum of the organization's policy on privacy and computer security in the employee manual.

Riddle (1990) attempts to sort out the legal responsibilities and rights of BBS administrators. He considers four key areas: 1) what, if any, role electronic bulletin boards might play as press, in terms of First Amendment rights; 2) what decision rules might apply to system operators concerning their liability for defamation when defaming material is posted by users; 3) other liability for message content; and 4) how search and seizure may or may not apply to electronic bulletin board services. Since state laws vary, though, the issues for bulletin board services remain problematic. The laws clearly are lagging far behind the technology.

Solutions to ethical problems, too, are slippery. Researchers, apart from legal considerations, are wrestling with the ethics and moral responsibilities of sampling text from public bulletin boards and mailing lists (e.g., ProjectH, 1992a; ProjectH, 1992b). One solution is to draw samples that e-mail recipients forward to the researcher, although the original sender may be unaware that the document is so used (e.g., Wambach, 1991). Although disguising identifiers may prevent recognition of the author, this approach does not address the questions of intellectual propriety or informed consent. Another solution (e.g., McCormick & McCormick, 1992) triangulates methods with logon warnings that the CMC is can be read by other parties as well as deleting all identifiers from the text. To date, however, ethical approaches are as varied as the number of researchers.

Big Brother is coming: the future of organizational monitoring

Organizational surveillance techniques are becoming more sophisticated every day. Marx (1992) reports that approximately 10 million employees are monitored in the United States every day, by phone, computer, or in person. He indicates that although many managers favor electronic means, citing increased productivity, accountability, and improved feedback, workers often feel "invaded, distrusted, and demeaned" (p. 29). Sloane (1992) and Coy (1992) report a new system that truly smacks of George Orwell's Big Brother. Here, a clip-on employee badge includes a microcomputer the size of an identification card that transmits signals to a central system. It reports the wearer's name, location, telephone extension, and time spent at a specific location. Sloane (1992) foresees that this may spur regulation of how much surveillance organizations can use and whether employees must be apprised of such monitoring, while Marx (1992) takes a more critical approach. He suggests that rather than "inflicting" such technology on the least powerful of organizational members, "greater potential damage" can be perpetrated by more powerful employees than those lower on the organizational ladder, and that

"fairness requires that the technologies inflicted on the most powerless...should also be used against the most powerful" (p. 29).

Flaming and fantasizing in cyberspace

Numerous scholars note the symbolic nature of electronic communication (e.g., Short, Williams, & Christie, 1976; Sitkin, Sutcliffe, & Barrios-Choplin, 1989). In fact, CMC systems usually support only a "low-end ASCII" character set. This means the communicator is limited to upper and lower case letters and numerals, and some commonly-used mathematical and punctuation symbols (e.g., "$," "%," "()," "+," etc.). Therefore, the sender and receiver must rely on a fairly narrow set of predetermined symbols with which they endeavor to create meaning.

As a form of interpersonal communication, all varieties of e-mail and public boards lack many cues that serve to regulate social interaction (Culnan & Markus, 1988, pp. 426-427). Here, the medium is the message, not in the McLuhan sense, but in Giddens' structurationist sense (e.g., Contractor & Eisenberg, 1990; Giddens, 1976; Poole & McPhee, 1983; Riley, 1983). The medium's symbolic meaning becomes both a product of and a constraint upon the communication process, as illustrated by the emergence of an infant "e-mail etiquette," (Shapiro & Anderson, 1985) complete with symbols and conventions that, while continually evolving, are largely accepted system-wide, and often inter-system. Abrasive, even abusive electronic communication is common enough to have been dubbed "flaming," a term unique to the medium.

Although electronic groups may consist of unseen members who do not occupy shared physical space and who interact asynchronously, Finholt and Sproull (1990) report that they tend to behave like social groups. Furthermore, communicators develop social alliances, and heavy users actually tend to form new friendships via computer-mediated means (e.g., Hellerstein, 1985). Some research indicates that people in computer-mediated groups may be less inhibited than in face-to-face groups, and that group members participate more equally than in face-to-face settings (Kiesler, Siegel, & McGuire, 1984). In other words, shared meaning in cyberspace seems to include unique user behaviors as group norms and practices emerge. In some cases, those behaviors are of a nature usually reserved for intimate encounters (e.g., examples cited in Furniss, 1993). The exchange of pornographic pictures, X-rated e-mail, and computer chats that are nothing less than sexual encounters are commonplace.

This speaks to the issue of caution (or lack of it) exercised by e-mail users. Lower inhibitions imply lower levels of caution. The question is whether these caution levels relate to user perceptions of privacy.

The review of literature suggests that many privacy issues stem from the fact that the content of messages is of a personal or embarrassing nature for the writer. But clearly, the computer is not a secure medium for private communication. And equally clearly, users who do

not practice "safe e-mail" are at risk of embarrassment or professional disaster. As the use of electronic mail increasingly replaces other channels of communication such as surface mail, telephone, and in-person meetings (Schaefermeyer & Sewell, 1988), resolution of these concerns becomes more critical. Why would users knowingly expose themselves to embarrassment, professional hazards, or even legal action by writing e-mail messages of a personal or compromising nature?

Such behavior appears similar to that of other high-risk behaviors in health or safety practices. Numerous studies show that, despite the risk of AIDS, individuals engage in unprotected sex, and scholars cite a variety of underlying factors, including risk-taking (Sherr, Strong, & Goldmeier, 1990), social or sexual anxiety (Hobfoll, Gayle, Gruber, & Levine, 1990), social responsibility (Baldwin & Baldwin, 1988), and nonpersonalization of risk (Edgar, Freimuth, & Hammond).

Similar studies concerning seatbelt usage consider gender differences (Tipton, Camp, & Hsu, 1990), and habits and attitudes (Mittal, 1988). One rather alarming study reports low rates of caregivers using car-restraint systems for infants one-to-two months of age, although automobile accidents create the number one cause of mortality and morbidity in children (Davis, 1985). It seems, then, that many people tend to ignore personal risks when it suits them to do so.

From a structurationist perspective, unguarded or cautionless communicative behavior in cyberspace may become (if it hasn't already) profoundly embedded in the network, thus becoming part of the structure, constraining it, producing it, and recreating it as it creates the discourse. Studies of user perceptions compared to the levels of risky communication may be illuminating, in terms of how widely spread such communication actually is, whether users lull themselves into a false sense of electronic security, and if risky CMC behaviors take place in spite of user awareness. Certainly, a variety of communication phenomena are at play in CMC. Some are shared with other media; others are unique to a medium that is dependent on computer and keyboard. All are inherent in a still-poorly understood medium that is evolving almost minute-by-minute, and offering communication scholars new opportunities for research with every new development.

References

Anderson, R.E., Johnson, D.G., Gotterbarn, D., & Perolle, J. (1993). Using the new ACM Code of Ethics in decision making. Communications of the ACM, 36(2). pp. 98-107.

Baird, R.E. (August 29, 1991). New questions emerge about computer crime: New computer technology creates new legal, ethical boundaries. Colorado Daily. Available via anonymous ftp. ftp.eff.org pub/cud/papers/rights.of.expr.

Baldwin, J.D. & Baldwin, J.I. (1988). Factors affecting AIDS-related sexual risk-taking behavior among college students. Journal of Sex Research, 25(2). pp. 181-196.

Burke, S. (August 20, 1990). Electronic-mail privacy to be tested in court in suit against Epson. PC Week, 7(33). p. 124.

Contractor, N.S. & Eisenberg, E.M. (1990). Communication networks and new media in organizations. In J. Fulk & C. Steinfeld, (Eds.). Organizations and Communication Technology. Newbury Park, CA: Sage Publications.

Coy, P. (August 17, 1992). Big Brother, pinned to your chest. Business Week. n3279, p. 38.

Culnan, M.J. & Markus, M.L. (1988). Information technologies. In G.A. Barnett & G.M. Goldhaber, (Eds.). Handbook of Organizational Communication. Norwood, NJ: Ablex Publishing Corporation. pp. 420-443.

Davis, D.J. (1985). Infant car safety: The role of perinatal caregivers. Birth: Issues in Perinatal Care & Education, 12. Supp. 3, Part 1, pp. 21-27

Edgar, T., Freimuth, V.S., & Hammond, S.L. (1988). Communicating the AIDS risk to college students: The problem of motivating change. Special Issue: AIDS. Health Education Research, 3(1). pp. 59-65.

Finholt, T. & Sproull, L.S. (1990). Electronic groups at work. Organizational Science, 1(1). pp. 41-64.

Francese, P. (1991). What business are you in. American Demographics, 13(4). p. 2.

Furniss, M. (1993). Sex with a hard (disk) on: Computer bulletin boards and pornography. Wide Angle, forthcoming.

Giddens, A. (1976). New Rules of Sociological Method: A Positive Critique of Interpretative Sociologies. New York: Basic Books.

Hellerstein, L.N. (1985). The social use of electronic communication at a major university. Special issue: Social impact of computers. Computers and the Social Sciences, 1(304). pp. 191-197.

Hernandez, R.T. (1987). Computer electronic mail and privacy. Paper written at California Wetern School of Law. Available via anonymous ftp: ftp.eff.org. pub/cud/papers/email-privacy.

Hobfoll, S.E., Gayle, J.A., Gruber, V., & Levine, O. (1990). Anxiety's role in AIDS prevention. Anxiety Research, 3(2). pp. 85-99.

Kahn, (1989). Defamation liability of computerized bulletin board operators and problems of proof. CHTLJ Comment. Available via anonymous ftp: ftp.eff.org. pub/cud/papers/.

Kapor, M. (1992). Computer spies. Forbes, 150(11). p. 288.

Keppel, B. (May 23, 1990). Electronic mail stirs debate on the privacy issue. Los Angeles Times, 109. p. D1.

Keubelbeck, A. (September 4, 1991). Getting the message. Los Angeles Times, 110. pp. E1-2.

Kiesler, S., Siegel, J. & McGuire, T. (1984). Social psychological aspects of computer-mediated communication. American Psychologist, 39(10). pp. 1123-1134.

Lewis, P.H. (December 23, 1990). On electronic bulletin boards, what rights are at stake? The New York Times, 140(3). p. F8

Loebl, J.W. (1992). Law firms, employees may clash over rights to computerized data. The national Law Journal, 14(9). p. 30.

Marx, G.T. (1992). Let's eavesdrop on managers. Computerworld, 26(16). p. 29.

McCormick, N.B. & McCormick, J.W. (1992). Computer friends and foes: Content of undergraduates' electronic mail. Computers in Human Behavior, 8. pp. 379-405.

Miller, M.W. (1991). Lotus is likely to abandon consumer-data project. The Wall Street Journal. January 23. p. B1.

Miller, S.C. (1992). Privacy in e-mail? Better to assume it doesn't exist. The New York Times, 151(3). pp. p8F(N), p8F(L).

Mittal, B. (1988). Achieving higher seat belt usage: The role of habit in bridging the attitude-behavior gap. Journal of Applied Social Psychology, 18(12). Pt. 2. pp. 993-1016.

Moore, W.J. (1992). Taming cyberspace. National Journal, 24(13). pp. 745-749.

Niven, D., Wang, C., Rowe, M.P., Taga, M, Vladeck, J.P., & Garron, L.C. (1992). The case of the hidden harassment. Harvard Business Review, 70(2). pp. 12-19.

Poole, M.S. & McPhee, R.D. (1983). A structural analysis of organizational climate. In L.L. Putnam & M.E. Pacanowsky (Eds.), Communication and Organizations: An Interpretive Approach. Beverly Hills: Sage, pp. 195-219.

ProjectH. (1992a). The great ethics debate. Available via anonymous ftp. arch.su.oz.au. pub/projectH/ethics/---six separate files.

ProjectH. (1992b). Ethics policy. Available via anonymous ftp. arch.su.oz.au. pub/projectH/ethics.

Ratcliffe, M. (1992). Privacy focus of Borland case. MacWeek, 6(35). pp. 1-2.

Reid, B. (August 6, 1993). Top 40 newsgroups in order by popularity (July 1993). Available via the Internet news group, news.lists.

Reynolds, C. (1990). Private and confidential. New Scientist, 127). p. 58.

Riddle, M.H. (1990). The electronic pamphlet--Computer bulletin boards and the law. Available via anonymous ftp. ftp.eff.org. pub/cud/papers/bbs.and.the.law.

Riley, P. (1983). A structurationist account of political culture. Administrative Science Quarterly, 28. pp. 414-437.

Schaefermeyer, M.J. & Sewell, E.H. (1988). Communicating by electronic mail. American Behavioral Scientist, 32(2). pp. 112-123.

Shapiro, N.Z. & Anderson, R.H. (1985). Toward an ethics and etiqueete for electronic mail. Paper prepared for the National Science Foundation. The Rand Corporation, Santa Monica, CA. Available via anonymous ftp. rand.org. /R-3283

Sherr, L., Strong, C., & Goldmeier, D. (1990). Sexual behaviour, condom use and prediction in attenders at sexually transmitted disease clinics: Implications for counselling. Special Issue: Sexual and marital counseling: Perspectives on theory, research and practice. Counselling Psychology Quarterly, 3(4). pp. 343-352.

Short, J., Williams, E., & Christie, B. (1976). The Social Psychology of Telecommunications. New York: Wiley.

Sitkin, S.B., Sutcliffe, K.M., Barrios-Choplin, J.R. (September 1989). Determinants of communication media choice in organizations: A dual function perspective. Paper presented at the 1989 National meeting of the Academy of Management, Washington, D.C.

Sloane, L. (September 12, 1992). Orwellian dream come true: A badge that pinpoints you. The New York Times, 141. pp. 14(N) & 11(L).

Smith, M.J. (1988). Contemporary Communication Research Methods. Belmont, CA: Wadsworth Publishing Company.

Solomon, J. (August 6, 1990). Electronic mail: Is it for your eyes only? The Wall Street Journal. p. B1.

Tipton, R.M., Camp, C.C., & Hsu, K. (1990). The effects of mandatory seat belt legislation on self-reported seat belt use among male and female college students. Accident Analysis & Prevention, 22(6). pp. 543-548.

Turner, J.A. (September 14, 1991). Messages in questionable taste on computer networks pose thorny problems for college administrators. Chronicle of Higher Education. January 24. p. A13.

Wallich, P. (1993). Electronic envelopes? The uncertainty of keeping e-mail private. Scientific American, 268(2). pp. 30-31.

Wambach, J.A. (1991). building electronic mail coalitions: Network politics in an educational organization. Paper presented at Western States Communication Association, Organizational Communication Interest Group, Phoenix, AZ.

White, G. (January 8, 1991). Suit says Nissan fired pair over privacy issue. Los Angeles Times, 110. p. D3